<u>REMARKS:</u>

Claims 1-12, 14-18, 20-35, 37-41 and 43-52 are presented for examination. Claims 1, 14, 18, 20, 26, 36, 41, 43, 49 and 50 have been amended hereby. Claims 51 and 52 have been added. Claims 13, 19, 36 and 42 have been cancelled, without prejudice or disclaimer.

As suggested by the Examiner at page 2 of the June 28, 2005 Office Action, the title of the application has been changed to "METHOD AND SYSTEM FOR MANAGING ACCESS TO INFORMATION AND THE TRANSFER THEREOF".

Further, as recommended by the Examiner at page 2 of the June 28, 2005 Office Action, the abstract has been changed to be more descriptive of the invention recited in the claims.

Further still, regarding the Examiner's indication at page 2 of the June 28, 2005 Office Action that the specification needs to be amended to include a "Brief Summary Of Invention," it is respectfully submitted that the relevant rules and regulations indicate that the specification <u>should</u> include such a "Brief Summary Of Invention" but <u>not</u> that the specification <u>must</u> include such a "Brief Summary Of Invention". Accordingly, it is believed that the structure of the specification meets the applicable requirements and that a "Brief Summary Of Invention" is not required.

Reconsideration is respectfully requested of the rejection of claims 18, 20-23, 41 and 43-46 under 35 U.S.C. 112, first paragraph.

Of note, only claims 18 and 41 were rejected under 35 U.S.C. 112, first paragraph, for substantive reasons (the other claims were rejected based on their dependency from claims 18 and 41)

In this regard, claims 18 and 41 have been amended to more clearly recite that the method and system further comprise "connecting to a plurality of intermediary servers" (thus being consistent with the recitation in the impendent claims of "an intermediary server").

Accordingly, it is respectfully submitted that the rejection of claims 18, 20-23, 41 and 43-46 under 35 U.S.C. 112, first paragraph, has been overcome.

Reconsideration is respectfully requested of the rejection of claims 18, 20-23, 41 and 43-46 under 35 U.S.C. 112, second paragraph.

Again, only claims 18 and 41 were rejected under 35 U.S.C. 112, second paragraph, for substantive reasons (the other claims were rejected based on their dependency from claims 18 and 41)

In this regard, claims 18 and 41 have been amended to more clearly claim this aspect of the invention by reciting "a plurality of intermediary servers" (rather than a "number of intermediary servers").

Accordingly, it is respectfully submitted that the rejection of claims 18, 20-23, 41 and 43-46 under 35 U.S.C. 112, second paragraph, has been overcome.

Reconsideration is respectfully requested of the rejection of claims 1-12, 14-16, 18, 20-22, 24-35, 37-39, 41, 43-45 and 47-50 under 35 U.S.C. 102(a) as allegedly being anticipated by U.S. Patent No. 5,923,756 ("Shambroom").

Initially, it is noted that applicant respectfully disagrees with the Examiner in the Examiner's analysis of the claims of the present application and the Shambroom disclosure.

Nevertheless, in order to expedite prosecution of the application, each of the independent claims has been amended hereby to more clearly distinguish over Shambroom by reciting that "access to specific information forming a subset of all information associated with the host server is dependent upon the distinct login authentication data transferred to the host server".

This controlled access feature (which had previously been included in claims 13 and 36) is discussed in the specification, for example, at page 13, line 13 to page 17, line 17. This controlled access feature is also shown graphically in Fig. 5, for example.

More particularly, as described in the specification at page 13, lines 13-17, one embodiment of a Context-sensitive Single Sign On ("CSSO") mechanism "may be provided for enabling a Network Service Provider to furnish external websites with the ability to securely authenticate a user to the Network Service Provider, <u>while restricting the user's access to only the set of information</u> that pertains to the external web site." (emphasis added)

It is respectfully submitted that despite the Examiner's comments made at page 6 of the June 28, 2005 Office Action, Shambroom simply fails to disclose, teach or suggest such a controlled access feature <u>in which access to specific information forming a subset of all information associated with the host server is dependent upon the distinct login authentication data transferred to the host server</u> (as recited in the claims).

In this regard, a studied review of the Shambroom disclosure was undertaken (with particular emphasis on Col. 9, lines 28-45 -- the portion cited by the Examiner as allegedly disclosing this feature). Below, for the Examiner's convenience, is a reproduction of the text of Col. 9, lines 28-45:

> The access indicator typically would include the Kerberos user principal name, a validity period, and a server session key for use between network server 300 and destination server 500, all of which has been encrypted with the private key of the destination server 500. KDC 400 then sends to network server 300 the encrypted access indicator, and a copy of the server session key encrypted using the KDC session key, as indicated at arrow 362.
>
> Thereafter, network server 300 decrypts the copy of the server session key that is encrypted using the KDC session key. Network server 300 then encrypts the message or command, using the server session key and, as indicated at arrow 364, sends the encrypted message along with the access indicator and a new authenticator to destination server 500 via insecure network 450. Destination server 500 uses its own private key to decrypt and obtain the server session key.
>
> By using the server session key, known only to destination server 500 and the network server 300, the authenticity of the identity of client 200 can be validated at destination server 500. The destination server 500 can then trust the integrity of the message, such as a command, from client 200, thereby permitting access to server 500 if validation is correct. Destination server 500 can compare the identity of client 200 to a list of access control criteria (ACL) that can be stored in ACL file 505 in destination server 500.

As seen from the above, the cited passage of Shambroom simply fails to disclose, teach or suggest the claimed access control feature.

In this regard, it appears that in Shambroom an "access indicator" is used to validate the authenticity of the identity of the client and that the destination server can compare the identity of the client to a list of "access control criteria". Of note, the portion of Shambroom cited by the Examiner does not elaborate on the functionality provided by the "access control criteria". However, such "access control criteria" is discussed again later in Shambroom at Col. 13, lines 4-8 (under the heading "Issuing A Command").

More particularly (and in keeping with the heading "Issuing A Command"), Shambroom indicates at Col. 13, lines 4-8 that "[t]he Secure Remote Execution Daemon 1290 also extracts access-control lists (ACLs) from ACL file 1330, and verifies that the Kerberos principal is authorized to execute the command as the specified user on Managed Host 1200. [Box 1516]".

Thus, while Shambroom may show, at most, verifying an authorization to execute a command as a specified user, the disclosure simply does not teach or suggest the claimed feature of controlling access to specific information forming a subset of all information associated with the host server.

Moreover, it is noted that under the claimed invention the aforementioned access control is carried out in dependence upon the distinct login authentication data transferred to a host server.

In contrast, it appears that the verification carried out by Shambroom is in connection with the execution of a command and not with login authentication data.

Accordingly, it is respectfully submitted that the rejection of claims 1-12, 14-16, 18, 20-22, 24-35, 37-39, 41, 43-45 and 47-50 under 35 U.S.C. 102(a) as allegedly being anticipated by Shambroom has been overcome.

Reconsideration is respectfully requested of the rejection of claims 17, 23, 40 and 46 under 35 U.S.C. 103(a) as allegedly being unpatentable over Shambroom in view of U.S. Patent No. 5,898,780 ("Liu et al.").

It is respectfully submitted that applicant does not necessarily concur with the Examiner in the Examiner's analysis of claims 17, 23, 40 and 46 of the present application and the Liu et al. reference.

For example, each of claims 17, 23, 40 and 46 recites (via a dependency upon a preceding claim) that the reviewed/modified/deleted document is included as part of the specific information subject to user access control in dependence upon the distinct login authentication data transferred to the host server.

In marked contrast, a review of the portion of Liu et al. cited by the Examiner (i.e., Col. 8, lines 26-59) reveals that what is discussed here is the writing of accounting data and the rewriting of configuration file changes. Of course, such accounting data and configuration files are not the same as the documents of the present invention which are subject to user access control in dependence upon the distinct login authentication data transferred to the host server.

Nevertheless, it is noted that each of claims 17, 23, 40 and 46 depends (directly or indirectly) from one of independent claims 1 and 26. Therefore, it is respectfully submitted that each of claims 17, 23, 40 and 46 is patentably distinct for at least the same reasons as the claim from which it depends.

Therefore, it is respectfully submitted that the rejection of claims 17, 23, 40 and 46 under 35 U.S.C. 103(a) as allegedly being unpatentable over Shambroom in view of Liu et al. has been overcome.

Turning now for a moment to new claims 51 and 52, it is noted that each of these claims depends (directly or indirectly) from one of independent claims 1 and 26. Therefore, it is respectfully submitted that each of claims 51 and 52 is patentably distinct for at least the same reasons as the claim from which it depends.

Moreover, it is noted that each of these claims 51 and 52 recites the feature directed to granting access to specific information in dependence upon which one of a plurality of intermediary servers the user had logged into.

In this regard, it is respectfully submitted that this feature additionally distinguishes over the cited references.

Finally, it is noted that this Amendment is fully supported by the originally filed application and thus, no new matter has been added. For this reason, the Amendment should be entered.

More particularly, support for the amendment of claims 1, 26, 49 and 50 regarding the access to specific information forming a subset of all information being dependent upon the distinct login authentication data transferred to the host server may be found in claims 13 and 36, as filed; in Fig. 5; at page 13, lines 13-17; and throughout the specification.

Further, support for the amendment of claims 18 and 41 regarding the plurality of intermediate servers may be found in claims 18 and 41, as filed; at page 16, lines 5-9; and throughout the specification.

Further still, support for new claims 51 and 52 regarding the plurality of intermediate servers may be found in claims 10 and 33, as filed; at page 16, lines 5-9; and throughout the specification.

Accordingly, it is respectfully submitted that each objection and rejection raised by the Examiner in the June 28, 2005 Office Action has been overcome and that the above-identified application is now in condition for allowance.

Respectfully submitted,
GREENBERG TRAURIG

Dated: December 28, 2005

By: ______________________
Matthew B. Tropper
Registration No. 37,457

Mailing Address:
GREENBERG TRAURIG
MetLife Building
200 Park Avenue
New York, NY 10166
(212) 801-2100
Facsimile: (212) 688-2449